На правах рукописи

Биричевский Алексей Романович

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПСЕВДОВЕРОЯТНОСТНОГО ПРЕОБРАЗОВАНИЯ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Специальность: 05.13.19 –
Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН)

Научный руководитель: доктор технических наук, профессор **Молдовян Николай Андреевич,** СПИИРАН

Официальные оппоненты: **Емелин Вадим Иванович,** доктор технических наук, старший научный сотрудник, главный научный сотрудник акционерного общества «Научно-исследовательский институт «Вектор», г. Санкт-Петербург

Татарникова Татьяна Михайловна, доктор технических наук, доцент, профессор кафедры безопасности информационных систем ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна»

Защита диссертации состоится “__” _____ 2017 г. в __ часов __ минут на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Россия, Санкт-Петербург, 14 линия, дом 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, www.spiiras.nw.ru.

Автореферат разослан “__” _____ 2017 г.

Ученый секретарь
диссертационного совета Д 002.199.01
доктор технических наук Кулешов Сергей Викторович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Большинство практических задач обеспечения информационной безопасности информационно-телекоммуникационных систем решается на программно-аппаратном уровне с использованием разнотипных операционных систем (ОС), хотя встроенные механизмы их функционирования являются весьма схожими. Встраивание в ОС механизмов аутентификации и защиты информации сокращает сроки и затраты на разработку прикладного программного обеспечения для мобильных устройств различного типа и назначения.

Средства алгоритмической защиты информации широко применяются на практике, однако их уязвимой частью является согласование параметров защитного преобразования взаимодействующими в ходе информационного обмена пользователями. Для перехвата этих параметров злоумышленник может применять принуждающие атаки, т.е. средства подкупа и специальные средства воздействия на пользователя. Для защиты пользователей от принуждающих атак предложено применение псевдовероятностного защитного преобразования. Интеграция псевдовероятностного защитного преобразования в подсистему защиты информации универсальной ОС обеспечит пользователю системы более высокий уровень защиты от принуждающих атак.

Данная работа посвящена решению актуальных научных и практических проблем: расширения функциональности средств защиты информации, обеспечения переносимости программных средств защиты информации на различные типы мобильных устройств (на различные типы технических платформ) и встраивания механизмов защиты от атак с принуждением.

Степень разработанности темы. Исследования методов обеспечения информационной безопасности операционных систем освещены в работах Зыль С., Махилёва В., Оладько А.Ю., Столлингс В., Шаньгина В.Ф., Безбогова А.А., Котенко И.В., Молдовяна А.А., Саенко И.Б., Лорина Г., Дейтеля Х.М. и др. Вопросы защиты информации от несанкционированного доступа освещены в работах Девянина П.Н., Семкина С.Н. и др.. Исследования в области разработки псевдовероятностных защитных преобразований приведены в работах Молдовяна Н.А., Щербакова В.А. и др.

Цель и задачи исследования. Цель данной работы состоит в сокращении сроков и уменьшении затрат по разработке защищенных мобильных информационных технологий за счет расширения функциональности и обеспечения переносимости программных средств защиты информации на различные типы мобильных устройств (на различные типы технических платформ) и встраивание механизмов защиты от атак с принуждением.

Для решения поставленной цели были сформулированы и решены следующие исследовательские **задачи:**

– выполнение анализа функциональных возможностей и особенностей реализации существующих мобильных операционных систем и на его основе разработка модели угроз информационной безопасности объекта исследования,

архитектуры и программного кода универсальной защищенной операционной системы для мобильных систем;

– разработка метода аутентификации пользователей стойкого к принуждающим атакам;

– разработка метода защитного преобразования передаваемой по открытым каналам информации, стойкого к атакам с принуждением пользователя раскрыть ключ защитного преобразования;

– разработка метода защиты программного обеспечения от дизассемблирования;

– разработка метода защиты хранимой информации**,** стойкого к атакам с принуждением пользователя раскрыть ключ защитного преобразования.

Научная новизна диссертационного исследования заключается в следующем:

1. Разработан метод аутентификации пользователей, отличающийся использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования.

2. Разработан метод защитного преобразования передаваемой по открытым каналам информации, отличающийся выполнением требования вычислительной неразличимости по шифртексту от вероятностного защитного преобразования.

3. Разработан метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода с помощью псевдовероятностного защитного преобразования машинного кода.

4. Разработан новый метод хранения ключей шифрования, отличающийся выполнением псевдовероятностного защитного преобразования ключей.

Теоретическая и практическая значимость работы. Теоретическая значимость работы состоит в разработке архитектуры универсальной защищенной мобильной ОС и новых алгоритмах защитных преобразований информации, обеспечивающих вычислительную неразличимость по шифртексту от вероятностного защитного преобразования. Практическая значимость состоит в том, что применение универсальной операционной системы в мобильных устройствах телекоммуникационных и информационных систем, в том числе в системах защиты информации, позволит унифицировать подходы к обеспечению безопасности при разработке таких систем. Данный подход упростит разработку и производство мобильных устройств. Область применения разработанной ОС включает разработку защищенных аутентифицирующих устройств (токенов, идентификаторов), систем охраны, устройств защиты программного обеспечения, персональных устройств хранения данных (защищенных файловых хранилищ), аппаратных средств для выполнения защитных преобразований данных.

Методология и методы исследования. В работе использован аппарат и методы математической статистики, теории вероятности, алгебры, теории чисел, криптографии и вычислительные эксперименты. *Объектом*

исследования являются мобильные операционные системы; *предметом* – способы, алгоритмы и протоколы обеспечения информационной безопасности в операционных системах.

Положения, выносимые на защиту:

1. Метод аутентификации пользователей по одноразовым паролям, обеспечивающий защиту от принуждающего несанкционированного доступа.
2. Метод защитного преобразования передаваемой по открытым каналам информации, обеспечивающий защиту от атак с принуждением к раскрытию ключа защитного преобразования.
3. Метод защиты программного обеспечения от активного и пассивного дизассемблирования, существенно повышающий вычислительную трудоемкость дизассемблирования машинного кода.
4. Метод хранения ключей шифрования обеспечивающий возможность сокрытия наличия резервных серий ключей.

Степень достоверности и апробация результатов. Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается анализом состояния исследований в данной области на сегодняшний день, формальными доказательствами, вычислительным экспериментом и апробацией результатов на всероссийской научно-практической конференции с международным участием «Комплексная защита объектов информатизации и измерительные технологии» (Санкт-Петербург, 16-18 июня 2014), юбилейной XIII Санкт-Петербургской международной конференции «Региональная информатика (РИ-2012)» (Санкт-Петербург, 24-26 октября 2012), VI межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных» (Брянск, 2014), VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)» (Санкт-Петербург, 23-25 октября 2013 г), IX Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2015)» (Санкт-Петербург, 28-30 октября 2015 г).

Результаты диссертационной работы внедрены в учебный процесс кафедры информационной безопасности Института точных наук и информационных технологий Сыктывкарского государственного университета на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

Основные результаты диссертации изложены в 12 публикациях, в том числе, в 3 статьях, опубликованных в ведущих рецензируемых журналах, входящих в перечень ВАК, в 3 докладах на международной конференции и 6 докладах на российских конференциях.

Структура и объем работы. Диссертационная работа изложена на 154 страницах, включает 4 главы, 38 рисунков, 7 таблиц и список литературы из 112 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована своевременность и актуальность темы диссертации, сформулированы цели исследования и решаемые задачи, определена научная новизна и приведено краткое содержание работы по главам.

В первой главе были рассмотрены особенности реализации мобильных операционных систем на примере ОС для смарт-карт. В каждой из представленных операционных систем были выделены особенности реализации. Основной функцией операционной системы для смарт-карт является обеспечение функционирования протоколов работы с картой, которые описаны в стандарте ISO/IEC 7816. Данные протоколы взаимодействуют с криптографическими контейнерами, которые могут храниться во внутренней (защищенной) памяти микроконтроллера. Для реализации защищенного хранилища криптографических контейнеров производители смарт-карт применяют два основных подхода:

– реализация смарт-карты на основе специализированного микроконтроллера,

– использование универсального микроконтроллера совместно с дополнительными мерами защиты.

Механизмы доступа к памяти также имеют важное значение. Так, например, операционная система MULTOS AG имеет в своем составе подсистему контроля использования ресурсов системы прикладными процессами. Многие производители концертирует ресурсы системы в файловой системе. Файловая система является наиболее удобной структурированной иерархической структурой, которая может включать в себя объекты различного типа (файлы, каталоги, ссылки на функции и т.д.). Реализация файловой системы в операционной системе MULTOS AG также имеет особенный интерес. В структуре файловой системы включены специализированный файловые объекты, такие как «цикличный файл».

На основе полученных данных об архитектуре существующих мобильных систем была построена модель угроз операционной системы для мобильных систем и поставлены научно-технические задачи исследования.

Вторая глава посвящена разработке методов аутентификации пользователей, контроля и управления доступом и методов активной защиты. Была рассмотрена подсистема разграничения доступа, которая является наиболее важной в составе операционной системы.

С целью повышения эффективности функционирования подсистемы аутентификации был разработан **метод аутентификации пользователей системы, обеспечивающий защиту принуждающей атаки** и алгоритмы, реализующие данный метод.

Подсистема аутентификации локальных пользователей обеспечивает классическую аутентификацию пользователей с использование многоразовых паролей, реализованную на основе разработанного алгоритма аутентификации пользователей с защитой от принуждающей атаки.

На первоначальном этапе алгоритма выбираются два имени пользователя, основное и резервное, с похожим названием (к примеру, user1 и userl) для нарушителя, выполняющего визуальное несанкционированное наблюдение процесса ввода пароля. Один пользователь имеет необходимые права в системе. Второй пользователь имеет минимальные права. В случае ввода резервного пароля (при принуждающей атаке) будет выполнен вход под именем пользователя, обладающего ограниченными правами доступа.

Процесс аутентификации начинается с запроса у пользователя логина и пароля. Далее необходимо вычислить ключ шифрования по формуле

$$K = h(login, pass),$$

где $K -$ ключи шифрования, $h(\,) -$хеш функция, $login -$ строка имени пользователя, $pass -$ строка пароля пользователя.

В операционной системе хранится файл хранилища шифртекстов. В данном файле хранится шифртекст C_{login},, сгенерированный на этапе регистрации пользователя. Далее необходимо расшифровать сообщение ключом, полученным на предыдущем шаге по формуле

$$M = D_K(C_{login}),$$

где M – расшифрованное сообщение, $D_K(\,)$–функция расшифрования.

Если сообщениеMсостоит из $login$" (возможно, отличного от введенного) и хеш-значения данного полученного $login$":

$$M = \{login" \mid h(login")\},$$

то необходимо осуществить вход в систему под пользователем $login$", иначе переход к первому шагу.

При вводе резервного пароля будет расшифровано значение резервного логина и пользователь выполнит вход под пользователем с усеченными правами.

В работе был разработан алгоритм аутентификации пользователей на одноразовых паролях с защитой от принуждающей атаки. За основу алгоритма был взят протокол аутентификации на одноразовых паролях S/KEY, который описан в стандарте интернета RFC1760.

На первом шаге пользователь выбирает парольную фразу P, вектор инициализации S - случайное число, которое позволяет использовать пользователю одну и ту же парольную фразу для нескольких серверов и два простых числа p_1, p_2. Далее производятся операции "исключающий ИЛИ" значений P и S. Вычисление временных паролей производятся по следующим формулам:

$$\begin{cases} \mathrm{K_N} = \mathrm{h(P\ xor\ S)}, \text{для } \mathrm{N} = 1 \\ \mathrm{K_N} = \mathrm{h(K_{N-1})}, \ \text{для } \mathrm{N} > 1' \end{cases}$$

где $\mathrm{h}(\,) -$ хеш функция, а N - количество генерируемых паролей.

Аналогично генерируются 2 списка из N паролей, при этом для каждого списка вектор инициализации также должен быть уникальный.

На сервере хранится файл криптографических значений, который содержит значения результатов шифрования. Выбирается случайное значение K_0 для первого криптографического значения C. Для генерации файла криптографических значений для N одноразовых паролей выбираются $2N$ случайных значений R. N криптографических значений вычисляются по формулам:

$$M_N = h(ID)|R_{1N}, \bar{M}_N = h(ID)|R_{2N};$$
$$K = R_{1(N-1)};$$
$$C_N = \left[{M_N}^{K_{11}} Kp_2(p_2^{-1} mod p_1) + {\bar{M}_N}^{K_{21}} Kp_1(p_1^{-1} mod p_2) \right] mod p_1 p_2,$$

где ID пользователя - уникальный идентификационный номер пользователя (Числовое значение).

Для получения последнего криптографического значения C используются следующие формулы:

$$M_1 = h(ID)|R_{12}, \bar{M}_1 = h(ID)|R_{22};$$
$$K = K_0;$$
$$C_1 = \left[{M_1}^{K_{1N}} Kp_2(p_2^{-1} mod p_1) + {\bar{M}_1}^{K_{2N}} Kp_1(p_1^{-1} mod p_2) \right] mod p_1 p_2.$$

На стороне клиента хранятся:

1) список из $2N$ паролей;
2) парольная фраза и 2 вектора инициализации (если необходима генерация паролей).

На стороне сервера хранятся:

1) файл криптографических значений (содержит N криптографических значений);
2) номер текущего пароля пользователя;
3) значения простых чисел p_1, p_2;
4) временный общий ключ K.

Использование одноразовых паролей начинается с последнего пароля (K_{1N}). Для дешифрования проверочного сообщения необходимо вычислить следующие значения:

$$M = (CK^{-1})^{K_{1N}^{-1}} \, mod \, p_1,$$
$$\bar{M} = (CK^{-1})^{K_{2N}^{-1}} \, mod \, p_2.$$

В первоначальном состоянии временный ключ $K = K_0$, а номер текущего пароля - 1. Для проверки одноразового пароля K_{1N} сервер производит дешифрование криптографического значения C_1 по следующей формуле:

$$M_1 = (C_1 K^{-1})^{K_{1N}^{-1}} \, mod \, p_1.$$

Стоит заметить, что, так как сервер не имеет сведений, какой серии пользователь предоставил пароль (K_{1N}или K_{2N}), серверу необходимо попробовать дешифровать значение, используя также и простое число p_2:

$$M_1 \neq (C_1 K^{-1})^{K_{1N}^{-1}} \, mod \, p_2.$$

В данном случае сервер не сможет дешифровать проверочное сообщение. Для проверки правильности проверочного сообщения сервер сравнивает первые 256 бит проверочного сообщения с вычисленным значением $h(ID)$. В случае удачной аутентификации в качестве временного общего ключа принимается расшифрованное значение R_{12} (аналогично производится завязка последовательности паролей).

В случае если пользователь передаст серверу пароль K_{2N}(при осуществлении вынуждающей отаки), проверка подлинности также пройдет успешно. Однако в качестве временного общего ключа будет принято неверное значение (а точнее значение R_{22}) и следующий пароль ($K_{1(N-1)}$или $K_{2(N-1)}$) будет признан неправильным.

Третья глава посвящена разработке методов защиты хранимой и передаваемой информации, стойких к атакам с принуждением пользователя раскрыть ключ защитного преобразования. В диссертации разработан **метод защитного преобразования информации и представлены построенные на его основе алгоритмы преобразований данных, обеспечивающих защиту от атак с принуждением.** Метод состоит в выполнении процедуры одновременного преобразования фиктивного и секретного сообщения по фиктивному и секретному ключу, в результате которой формируется единый шифртекст, расшифровывание которого может быть выполнено по отдельности по фиктивному ключу и по секретному ключу, причем каждый бит шифртекста влияет на результат расшифровывания в каждом из этих двух случаев. Метод включает формирование двух промежуточных шифртекстов, представляющих собой результат шифрования фиктивного сообщения по фиктивному ключу и секретного сообщения по секретному ключу. После этого выполняется процедура отображения пары промежуточных шифртекстов в выходной шифртекст, размер которого равен сумме размеров промежуточных шифртекстов. Конкретная реализация метода в виде конкретных алгоритмов отрицаемого шифрования задается выбором алгоритмов формирования промежуточных шифртекстов. Описанный общий метод отрицаемого шифрования может быть реализован в виде частных методов, задаваемых вариантом выбора алгоритма преобразования промежуточных шифртекстов в единый выходной шифртекст, получаемый в результате отрицаемого шифрования.

Рассмотрим реализацию варианта метода, включающего решение системы линейных сравнений как способа выполнения преобразования промежуточных шифртекстов, на примере следующего алгоритма алгебраического псевдовероятностного защитного преобразования, который

начинается с генерации секретного ключа в виде набора подключей K_1, K_2, K_3, K_4 (K_1, K_2 для основного сообщения, K_3, K_4 для «фальшивого» сообщения) и двух простых чисел p_1 и p_2. Шифрование блоков M ($p_1 > M$) и $\overline{M}$ ($p_2 > \overline{M}$) двух сообщений осуществляют путем вычисления значения C_1 по формуле $C_1 = M^{K_1} K_2 \bmod p_1$, вычисления значения C_2 по формуле $C_2 = \overline{M}^{K_3} K_4 \bmod p_2$ и формирования блока криптограммы C, которое является решением системы сравнений

$$\begin{cases} C \equiv C_1 \bmod p_1 \\ C \equiv C_2 \bmod p_2 \end{cases},$$

которую можно представить в виде

$$\begin{cases} C \equiv M^{K_1} K_2 \bmod p_1 \\ C \equiv \overline{M}^{K_3} K_4 \bmod p_2 \end{cases}.$$

В соответствии с китайской теоремой об остатках решение вычисляется по следующей формуле:

$$C = \left[M^{K_1} K_2 p_2 \left(p_2^{-1} \bmod p_1 \right) + \overline{M}^{K_3} K_4 p_1 \left(p_1^{-1} \bmod p_2 \right) \right] \bmod p_1 p_2 .$$

При вынуждающей атаке необходимо предоставить атакующему одно из сообщений. Пусть в качестве "ложного" сообщения выступает $\overline{M}$. Тогда атакующему предоставляется в качестве ключа шифрования тройка значений K_3, K_4, p_2. Расшифрование выполняется по формуле

$$\overline{M} = \left(C K_4^{-1} \right)^{K_3^{-1}} \bmod p_2 .$$

В последней формуле обратные значения для подключей K_3 и K_4 вычисляются по модулям $p_2 - 1$ и p_2, соответственно. При необходимости расшифрования "истинного" секретного сообщения M выполняется вычисления по той же формуле, но с использованием ключа, представляющего собой тройку значений (K_1, K_2, p_1):

$$M = \left(C K_2^{-1} \right)^{K_1^{-1}} \bmod p_1 .$$

Для случая использования блочных шифрующих функций предложен метод выполнения защитных преобразований, состоящий в формировании блоков шифртекста, которые по фиктивному ключу расшифровываются в знаки фиктивного сообщения, а по секретному ключу в знаки секретного сообщения. При этом для выполнения процедуры расшифровывания фиктивного и секретного сообщений используется одна и та же функция блочного шифрования, а размер знаков сообщений меньше размера блоков шифртекста.

Данный метод положен в основу следующего алгоритма псевдовероятностного защитного преобразования на основе блочных защитных преобразований, удовлетворяющий критерию вычислительной неразличимости от вероятностного шифрования. Представленная на рисунке 1 блок-схема предложенного алгоритма псевдовероятностного защитного преобразования на основе блочных защитных (шифрующих) преобразований содержит следующие основные этапы:

Шаг 1. Установить значение счетчика шифруемых пар символов $i = 1$.

Шаг 2. Установить значение счетчика числа попыток подбора подходящего случайного значения$j = 1$.

Шаг 3. Сгенерировать случайное k-битовое число r_j.

Шаг 4. Вычислить значение $c_j = E_{K_M}(m_i, r_j)$.

Шаг 5. Вычислить значение $D_{K_T}(c_j) = (t_j, r'_j)$, где выходное n-битовое значение функции расшифрования интерпретируется как конкатенация u-битового значения t_j и k-битового значения r'_j.

Шаг 6. Сравнить значения t_j и t_i. Если $t_j = t_i$, то взять в качестве значения c_i значение c_j и перейти к шагу 7, в противном случае перейти к шагу 6.

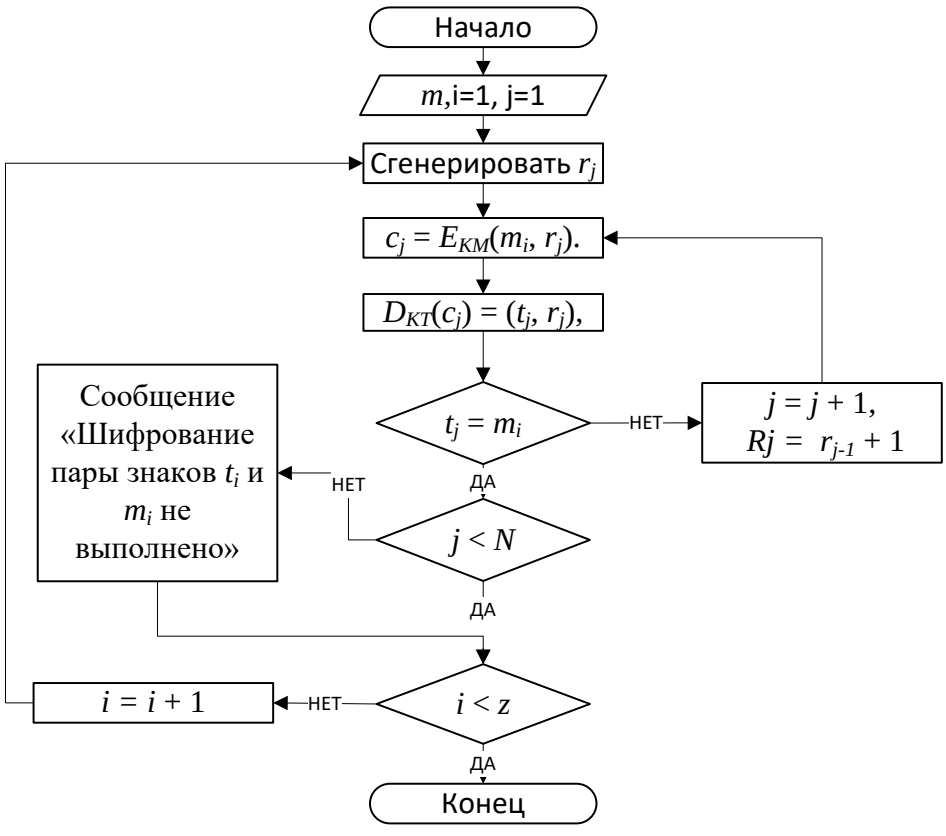

Рис. 1. Блок-схема алгоритма псевдовероятностного защитного преобразования на основе блочных шифрующих преобразований

Шаг 7. Если $j < N$, то прирастить значение счетчика $j \leftarrow j + 1$, вычислить $r_j \leftarrow r_{j-1} + 1$ и перейти к шагу 4, иначе вывести сообщение «Шифрование пары знаков t_i и m_i не выполнено».

Шаг 8. Если $i < z$, то прирастить значение счетчика $i \leftarrow i + 1$ и перейти к шагу 2, иначе СТОП.

Так как предложенный алгоритм использует функцию блочного шифрования (например, алгоритм ГОСТ28147-89 в режиме простой замены), процедура расшифрования алгоритма очень проста. Для расшифрования блока шифртекста применяется процедура расшифрования согласно спецификации применяемой функции блочного шифрования (в нашем примере, процедура расшифрования ГОСТ28147-89). В результате выполнения процедуры расшифрования получаем знак t_i, если использован ключ K_T, или знак m_i, если использован ключ K_M. Расшифрование всех блоков шифртекста по ключу K_T восстанавливает сообщение T, а по ключу K_M – сообщение M. При этом легко доказать, что шифртекст, полученный с помощью разработанного алгоритма псевдовероятностного защитного преобразования, может быть получен путем вероятностного шифрования сообщение M по ключу K_M. То есть предложенный алгоритм является алгоритмом псевдовероятностного защитного преобразования, поскольку он по шифртексту является вычислительно неотличимым от алгоритма вероятностного шифрования. Производительность предложенного алгоритма для блочного шифра $\lambda_{БШ}$ равна

$$\lambda_{ОШ} \approx (2^{-2u-1}u/n)\lambda_{БШ},$$

где $\lambda'_{ОШ}$ – скорость алгоритма-аналога;

$\lambda_{БШ}$– скорость базового блочного алгоритма шифрования;

u – битовая разрядность символов шифруемых сообщений;

n – разрядность входного блока данных для функции блочного шифрования.

Повышение скорости отрицаемого шифрования в 2^{-u} раза, обеспечиваемое разработанным алгоритмом по сравнению с алгоритмом аналогом, достигнуто за счет существенного уменьшения среднего числа попыток подбора в механизме, положенным в основу процесса отрицаемого шифрования.

Для проверки теоретических данных были выполнены вычислительные эксперименты по оценке значения η (число пробных выборок), которые подтвердили теоретическое значение $\eta = 2u$. Рисунок 2 иллюстрирует экспериментальные данные.

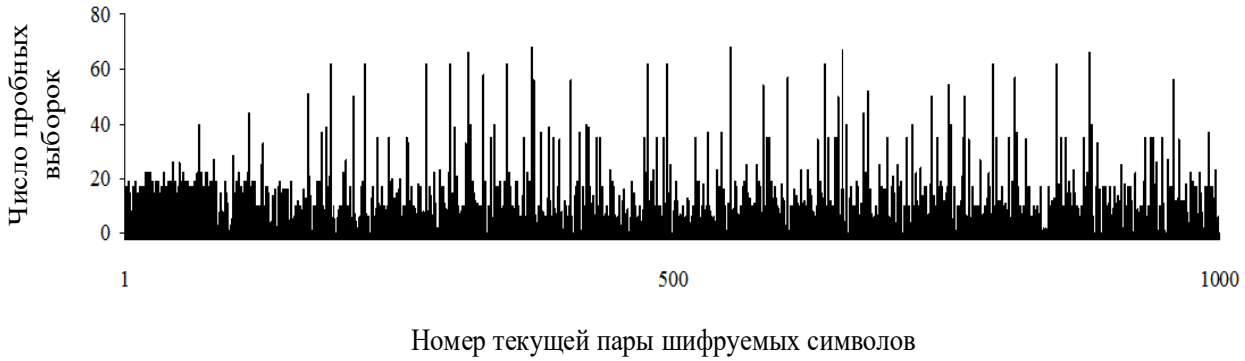

Рис. 2. График зависимости числа пробных выборок значения rj от номера текущей пары шифруемых символов при использовании блочного шифра ГОСТ 28147 и параметров $u = 4$, $n = 64$.

Эксперимент подтвердил, что ощутимое влияние на скорость выполнения раунда отрицаемого шифрования оказывает размер блока данных (значение u). Вероятность совпадения 4 бит (шаг 1.6 алгоритма) выше вероятности совпадения 8 бит.

В четвертой главе описывается модель разработанной защищенной операционной системы для мобильных систем. Для выполнения отладки и испытаний разработанной операционной системы были спроектированы отладочные аппаратные платформы (макетные стенды). Стенды имитируют некоторые распространенные классы средств защиты информации, в том числе:

– криптографическое хранилище информации,

– персональное идентифицирующее устройство для интерфейса USB (USB-токен).

Макетные стенды разрабатывались с учетом специфики использования устройств и нововведений в микроэлектронике.

В подсистеме информационной безопасности разработанной операционной системы также было применено псевдовероятностное преобразование. Для защиты приложений в ОС был разработан **метод защиты программного обеспечения от активного и пассивного дизассемблирования**, основанный на введении ложных веток кода с помощью псевдовероятностного защитного преобразования кода.

Наиболее часто используемой в коде программных продуктов структурой является «условие». «Условие» используется как самостоятельно, так и в более сложных структурах, таких как «цикл».

Для защиты от статического анализа (дизассемблирования) целесообразно в ключевых блоках программы вместо структуры «условие» использовать псевдовероятностное защитное преобразование. На рисунке 3 изображена блок-схема функции, которая в качестве конструкции типа «условие» использует блок шифрования.

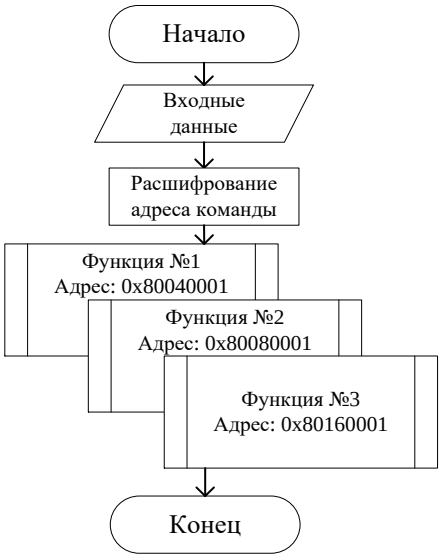

Рис. 3. Использование псевдовероятностного защитного преобразования в качестве конструкции типа «если»

Вместо ключа используются входные данные блока «условие». На выходе необходимо реализовать ложные ветви кода (например, в зашифрованном сообщении может содержаться адрес следующей блока программы). Такая структура (далее - блок шифрования) применяется и в других методах защиты от анализа, которые будут описаны далее. На вход блока шифрования будет подаваться параметр (ключ). На выходе блока будет получен адрес следующей команды (открытый текст).

Результат выполнения блока «если» может содержать любое количество адресов ветвей кода истинных или ложных. При этом для злоумышленника последующее выполнение каждой из ветвей кода будет равновероятно.

Применение псевдовероятностного защитного преобразования в качестве конструкции типа «условие» позволит значительно усложнить (особенно при многократном применении) статический анализ приложения (дизассемблирование).

Для защиты программы от активного анализа средствами отладки, также может применяться псевдовероятностное преобразование.

Один из способов применения псевдовероятностного защитного преобразования для контроля времени - контроль времени выполнения.

На входе блока шифрования: разница во времени (например, может быть передано количество тактов процессора, которое прошло за период времени).

На выходе блока шифрования: адрес следующего блока основной программы (либо ложной ветви алгоритма).

Второй способ применения псевдовероятностного защитного преобразования для контроля времени - контроль момента времени выполнения.

На входе блока шифрования: настоящее время.

На выходе блока шифрования: адрес следующего блока основной программы (либо ложной ветви алгоритма).

Такая стратегия может также быть применена также в пробных версиях программных продуктов (например, для работы программы в течение конкретного месяца).

В работе был предложен **метод хранения ключей шифрования, отличающийся выполнением псевдовероятностного защитного преобразования ключей**. В данном методе для сокрытия наличия резервных серий ключевой информации предложено применять псевдовероятностное преобразование. Далее описан алгоритм применения отрицаемого шифрования для хранения ключей, реализующий вышеуказанный метод. На рисунке 4 представлен пример применения алгоритма псевдовероятностного преобразования для хранения набора резервных серий ключевой информации.

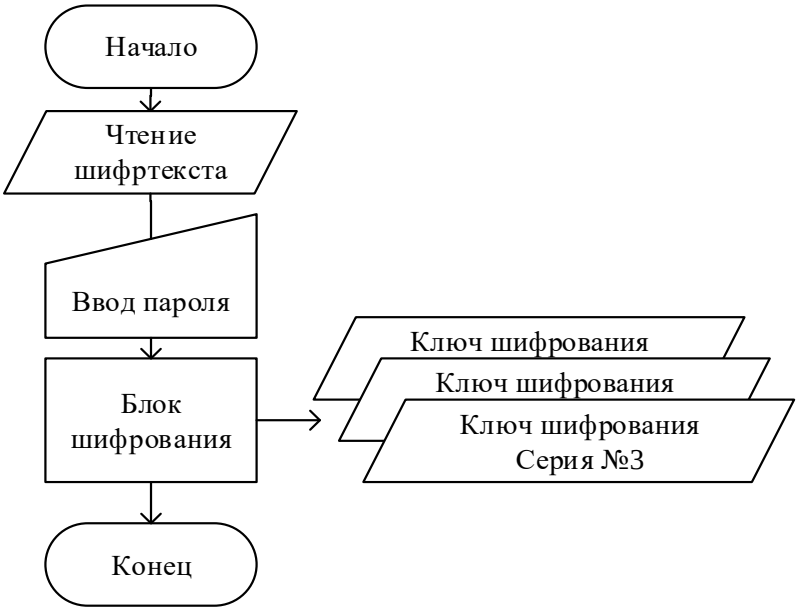

Рис 4.Схема алгоритма использования отрицаемого шифрования для хранения резервных серий ключевой информации

Контейнер ключей представляет собой файл, который содержит в себе значение шифртекста *C*. Для вычисления данного значения для n серий ключей необходимо найти решение системы уравнений:

$$\begin{cases} E_{K1}(C)\ mod\ 2^r = M_1, \\ \dots \\ E_{Kn}(C)\ mod\ 2^r = M_n, \end{cases}$$

где $K_1 \dots K_n -$ ключи шифрования ключей (пароль фиксированной длины); $M_1 \dots M_n -$ защищаемые серии ключей; $E -$функция шифрования; $C -$ криптограмма; r-разрядность криптограммы. Информация о наличии резервных серий ключевой информации может иметь значительную ценность для злоумышленника. В качестве алгоритма шифрования применяется ГОСТ 28147-89. Так как длина файла шифртекста не зависит от количества

зашифрованных серий ключевой информации, у злоумышленника отсутствует возможность доказать, что существуют несколько серий ключей.

Дополнительной положительной особенностью данного способа хранения ключевой информации является возможность совместить процесс генерации ключевой информации и выработки файла контейнера ключей.

В данном случае вычисление сводится к нахождению n значений ключей шифрования ключей $K_1 \dots K_n$ по формуле

$$E_{Kn}(C)\ mod\ 2^r = M_n.$$

Стоит отметить, что данный способ генерации можно применять только с учетом требований целевых алгоритмов шифрования для ключевой информации.

Представленный алгоритм применения псевдовероятностного преобразования для хранения ключевой информации позволяет обеспечить сокрытие самого факта наличия резервных серий ключевой информации. Данный алгоритм может быть применен в средствах прикладного шифрования.

ЗАКЛЮЧЕНИЕ

В ходе диссертационного исследования решена важная научно-техническая задача встраивания механизмов защиты информации на различные типы мобильных устройств за счет разработки методов и алгоритмов псевдовероятностного защитного преобразования, в том числе получены следующие основные научные и практические результаты:

1. разработан метод аутентификации пользователей с использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования, который обеспечивает защиту от принуждающих атак;
2. разработан метод псевдовероятностного защитного преобразования информации, обеспечивающий защиту информации от несанкционированного доступа в случае атак с принуждением;
3. разработан метод защиты программного обеспечения от дизассемблирования, основанный на введении ложных веток кода с помощью псевдовероятностного защитного преобразования кода;
4. разработан метод хранения ключей шифрования, основанный на применении псевдовероятностного защитного преобразования для обеспечения возможности сокрытия наличия резервных серий ключей.

Перспективы развития выполненного исследования состоят в разработке новых механизмов защиты информации от несанкционированного доступа, основанных на псевдовероятностных защитных преобразованиях, а также новых способов и алгоритмов, реализующих преобразования такого типа и обладающих более высокой производительностью.

Выполненное исследование и полученные результаты **соответствуют пп. 1, 2, 5, 6, 11 и 13 пунктов паспорта специальности 05.13.19**:

– теория и методология обеспечения информационной безопасности и защиты информации;

– методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида;

– методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

– модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования;

– технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа;

– принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в журналах, входящих в перечень ВАК:

1. **Молдовян Н. А., Биричевский А. Р., Мондикова Я.А**. Отрицаемое шифрование на основе блочных шифров // Информационно управляющие системы. № 5. 2014. С. 80-86.

2. **Биричевский А.Р., Молдовян Н.А., Березин А.Н., Рыжков А.В.,** Способ отрицаемого шифрования. // Вопросы защиты информации: Науч.-практ. журн. Москва:ФГУП "ВИМИ", 2013. Вып. 2 (101). С. 18-21.

3. **Биричевский А.Р.** Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования // Труды СПИИРАН. СПб.: Наука, 2016. №3. С.128-138.

Другие публикации:

1. **Биричевский А.Р.** Подход к обеспечению безопасности взаимодействия процессов при разработке операционных систем. Информационная безопасность регионов России (ИБРР-2013). И 74 VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. С. 49-50.

2. **Березин А.Н., Биричевский А.Р., Молдовян Н.А.** Особенности задачи дискретного логарифмирования по составному модулю как криптографического примитива // Труды VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011)». Санкт-Петербург, 26-28 октября. СПб.: СПОИСУ, 2012. С. 104-108.

3. **Биричевский А.Р., Мирин А.Ю., Молдовян Н.А.** Нетрадиционные приложения блочных шифров // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2011. С. 72-76.

4. **Биричевский А.Р., Молдовян Н.А., Рыжков А.В.** Отрицаемое шифрование как механизм защиты информации, хранимой на удаленных носителях // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2011. С. 77-81.

5. **Березин А.Н., Биричевский А.Р., Мондикова Я.А.** Отрицаемое шифрование для защиты информации от НСД // 5-я научно-практическая конференция "Информационная безопасность. Невский диалог". Санкт-Петербург, 12-13 ноября 2013 г. / СПб.: «Студия «НП-Принт». С. 21-22.

6. **Биричевский А.Р.** Отрицаемое шифрование как механизм защиты приложений от отладки // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 21-22 ноября 2013, г. Санкт-Петербург / СПб.: ВАС, 2013. С. 81-85.

7. **Биричевский А.Р.** Практическое применение алгоритмов отрицаемого шифрования // Информационная безопасность и защита персональных данных: Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VI Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской. – Брянск: БГТУ,2014. С. 17-18.

8. **Биричевский А.Р.** Отрицаемое шифрование как механизм защиты приложений от отладки // Комплексная защита объектов информатизации и измерительные технологии: сб. науч. тр. Всероссийской науч.- практической конф. с международным участием. 16-18 июня 2014. -СПб.: Изд-во Политех. ун-та, 2014 С. 8-12.

9. **Биричевский А.Р.** Способ применения отрицаемого шифрования для хранения ключей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. С. 98-99.